

CLAIMS

What is claimed is:

- Sub
a1
- 1 1. A method for providing network security features, comprising the steps of:
 - 2 (a) identifying a plurality of network objects;
 - 3 (b) retrieving rule sets associated with at least one of the identified network
4 objects, the rule sets including a plurality of policy rules that govern actions
5 relating to the identified network objects;
 - 6 (c) reconciling overlapping policy rules of the rule sets amongst the network
7 objects; and
 - 8 (d) executing the reconciled rule sets.
 - 1 2. The method as recited in claim 1, wherein each policy rule of the reconciled
2 rule sets includes a rule action selected from the group consisting of:
3 permitting an action relating to the identified network objects, denying an
4 action relating to the identified network objects, and conditionally denying an
5 action relating to the identified network objects.
 - 1 3. The method as recited in claim 2, wherein an action relating to the identified
2 network objects is permitted if no policy rules deny the action, at least one
3 policy rule conditionally denies the action, and at least one policy rule
4 permits the action.
 - 1 4. The method as recited in claim 2, wherein the policy rules denying the action
2 are evaluated first, the policy rules conditionally denying the action are
3 evaluated second, and the policy rules permitting the action are evaluated
4 third.

- 1 5. The method as recited in claim 1, wherein an action relating to the identified
2 network objects is denied if none of the policy rules permit the action.
- 1 6. The method as recited in claim 1, wherein an action relating to the identified
2 network objects is denied if none of the policy rules match a request for the
3 action.
- 1 7. The method as recited in claim 1, wherein executing the reconciled rule sets
2 includes combining the rule sets into a single rule set.
- 1 8. The method as recited in claim 1, further comprising removing duplicate
2 policy rules of the rule sets.
- 1 9. The method as recited in claim 1, further comprising notifying a user of
2 conflicting policy rules of the rule sets.
- 1 10. The method as recited in claim 1, wherein the rule sets are associated with a
2 particular network object.
- 1 11. The method as recited in claim 1, wherein a protocol configuration enforced
2 by a related proxy is selected from a hierarchal list if an action is permitted
3 by more than one rule.
- 1 12. A computer program product for providing network security features,
2 comprising:
3 (a) computer code for identifying a plurality of network objects;
4 (b) computer code for retrieving rule sets associated with at least one of the
5 identified network objects, the rule sets including a plurality of policy rules
6 that govern actions relating to the identified network objects;
7 (c) computer code for reconciling overlapping policy rules of the rule sets
8 amongst the network objects; and

9 (d) computer code for executing the reconciled rule sets.

1 13. The computer program product as recited in claim 12, wherein each policy
2 rule of the reconciled rule sets includes a rule action selected from the group
3 consisting of: permitting an action relating to the identified network objects,
4 denying an action relating to the identified network objects, and conditionally
5 denying an action relating to the identified network objects.

1 14. The computer program product as recited in claim 13, wherein an action
2 relating to the identified network objects is permitted if no policy rules deny
3 the action, at least one policy rule conditionally denies the action, and at least
4 one policy rule permits the action.

1 15. The computer program product as recited in claim 13, wherein the policy
2 rules denying the action are evaluated first, the policy rules conditionally
3 denying the action are evaluated second, and the policy rules permitting the
4 action are evaluated third.

1 16. The computer program product as recited in claim 12, wherein an action
2 relating to the identified network objects is denied if none of the policy rules
3 permit the action.

1 17. The computer program product as recited in claim 12, wherein an action
2 relating to the identified network objects is denied if none of the policy rules
3 match a request for the action.

1 18. The computer program product as recited in claim 12, wherein executing the
2 reconciled rule sets includes combining the rule sets into a single rule set.

1 19. The computer program product as recited in claim 12, further comprising
2 computer code for removing duplicate policy rules of the rule sets.

1 20. The computer program product as recited in claim 12, further comprising
2 computer code for notifying a user of conflicting policy rules of the rule sets.

1 21. The computer program product as recited in claim 12, wherein the rule sets
2 are associated with a particular network object.

1 22. The computer program product as recited in claim 12, wherein a protocol
2 configuration enforced by a related proxy is selected from a hierarchal list if
3 an action is permitted by more than one rule.

1 23. A rule based network security system for providing network security
2 features, comprising:
3 (a) logic for identifying a plurality of network objects;
4 (b) logic for retrieving rule sets associated with at least one of the identified
5 network objects, the rule sets including a plurality of policy rules that govern
6 actions relating to the identified network objects;
7 (c) logic for reconciling overlapping policy rules of the rule sets amongst the
8 network objects; and
9 (d) logic for executing the reconciled rule sets.

1 24. A method for establishing network security, comprising the steps of:
2 (a) providing a plurality of network objects of a network and a plurality of rule
3 sets; and
4 (b) associating the network objects with the rule sets;
5 (c) wherein the rule sets include a plurality of policy rules that govern actions
6 relating to the identified network objects during operation of the network.

1 25. The method as recited in claim 24, wherein a user is allowed to associate the
2 network objects with the rule sets via a graphical user interface.

1 26. The method as recited in claim 24, wherein each policy rule of the reconciled
2 rule sets includes a rule action selected from the group consisting of:
3 permitting an action relating to the identified network objects, denying an
4 action relating to the identified network objects, and conditionally denying an
5 action relating to the identified network objects.

1 27. The method as recited in claim 26, wherein an action relating to the
2 identified network objects is permitted if no policy rules deny the action, at
3 least one policy rule conditionally denies the action, and at least one policy
4 rule permits the action.

1 28. The method as recited in claim 24, wherein an action relating to the
2 identified network objects is denied if none of the policy rules permit the
3 action.

1 29. A computer program product for establishing network security, comprising:
2 (a) computer code for providing a plurality of network objects of a network and
3 a plurality of rule sets; and
4 (b) computer code for associating the network objects with the rule sets;
5 (c) wherein the rule sets include a plurality of policy rules that govern actions
6 relating to the identified network objects during operation of the network.

1 30. The computer program product as recited in claim 29, wherein a user is
2 allowed to associate the network objects with the rule sets via a graphical
3 user interface.

1 31. The computer program product as recited in claim 29, wherein each policy
2 rule of the reconciled rule sets includes a rule action selected from the group
3 consisting of: permitting an action relating to the identified network objects,
4 denying an action relating to the identified network objects, and conditionally
5 denying an action relating to the identified network objects.

1 33. The computer program product as recited in claim 29, wherein an action
2 relating to the identified network objects is denied if none of the policy rules
3 permit the action.